Information Security and Business Continuity Planning for Archer Saas Offering, Archer Engage, And Archer Insight

Any capitalized terms used but not defined herein shall have the meaning set forth in the agreement between Archer and Customer that references this document. Archer may review and update its security obligations in this addendum, provided that such updates do not materially diminish the protections herein.

Organizational Security Measures

(see below for security measures specific to the Archer SaaS Service Offering)

1. Measures to ensure security of processing.

1.1. Entrance Control. Where appropriate, the following measures designed to prevent unauthorized persons from gaining access to data processing systems are used:

- Where visitors are permitted at data centers used to process customer-provided data, visitors must register the following information: full name of visitor; date and time of arrival; and purpose of visit.
- Data center access is granted on a least-privilege, and need-to-know basis.
- CCTV covers appropriate areas (e.g., entrances to data centers and other sensitive data center areas).
- The Archer corporate facility is secured by an access control system where access to the corporate facility is granted with an activated entry card or other appropriate technological measures.
- Outside areas may be under video surveillance or under monitoring by a security service or under guard service.

1.2. Admission Control. Appropriate measures preventing unauthorized persons from using data processing systems.

- Access to Archer-controlled IT systems is granted only to users when registered under authorized usernames.
- Internal password policy aligns to NIST SP 800-63B guidelines, or its successor.
- Archer corporate policy includes automatic computer lock after a short, technologically enforced period, with renewed access to the PC only after new registration with a valid username and password.
- Outside network access requires a two-factor-authentication.

1.3. Access Control. Appropriate measures to ensure that data cannot be read, copied, modified, or removed without authorization while processing or use and after storage, are as follows:

- Access authorization is issued in respect of the specific area of work to which the resource is assigned (work roles); and
- Policy requires regular verification of access authorizations.

1.4. Separation Control. Appropriate measures ensuring that data collected for different purposes can be processed separately:

- Data of different controllers shall be processed separately; and
- Functional separation between test and production systems is employed.

2. Measures to ensure integrity of processing.

2.1. Transmission Control. Appropriate measures to ensure that data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport are as follows:

- Encrypted data transfer when handling data and when accessing the company network.
- Monitoring of data transfer for suspicious traffic.
- Restrictive usage of Wireless LAN.
- Wireless networking is not leveraged in the provision of Archer cloud-based services.
- Restrictive remote access to Archer corporate network and systems (using two-factor-authentication).
- Where applicable, data media is disposed of in accordance with data protection policies by use of one or more of the following, as appropriate: safety containers and document shredders; physical destruction; erasure using industry standard processes; crypto shredding; or other approved disposition procedures.

- Remote support (screen sharing) requires an affirmative action from the recipient of the screen share request.

2.2. Input Control. Measures to ensure the identity and authorization associated with input, access, modification, and removal of data with respect to data processing systems are as follows:

- When using relevant applications, access is automatically recorded; and
- Remote support (screen sharing) permits the recipient of the screen share request to terminate the support activity at any time.

3. Measures to ensure security, availability, and resilience of processing.

3.1. Background Checks. No Processing according to Art. 28 GDPR shall take place without Controller's instructions, clear contract drafting, formalized assignment management, strict vetting processes, and checks. In addition:

- Subcontractors are on-boarded using processes that entail risk assessment, and implementation of contractual terms entailing data protection, confidentiality, integrity, and availability obligations, as appropriate.
- Subcontractors are regularly reviewed for compliance.
- To the extent legally permissible, Archer ensures that background checks are conducted on its employees at the onboarding stage.

3.2. Data protection measures. Measures to ensure that data is protected from accidental destruction or loss, are as follows:

- Where appropriate, anti-malware software is installed on applicable systems.
- Firewalls or equivalent technologies (e.g., AWS security groups) are used to protect Archer-controlled networks.
- Network segmentation is used where applicable and appropriate.
- Content filtration (e.g., proxies) are implemented for the Archer corporate network.
- Interruption-free power supply is required for all critical systems.
- Fire safety systems are in place where required by law.
- Processes or mechanisms for handling emergencies and disasters are in place and communicated to personnel responsible for handling such.

3.3. Resiliency. Where appropriate, punctual peak demands or long-term high demands are reflected in the design of systems and services (e.g., memory, access, and throughput capacities, etc.) to ensure resilience and consistency of processing.

3.4. Incident Response. Corporate response capabilities related to cybersecurity incidents are in place to address incident scope, identification, assessment, response, and remediation, including notifications to regulators, controllers, and/or data subjects, as may be required.

3.5. Encryption at rest. Data is encrypted at rest using current industry standard encryption techniques, ciphers, and strengths.

3.6. Testing. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing are as follows:

- Corporate security policies are reviewed at least annually, with final review/approval provided by the Chief Information Security Officer.

Information Security Protections for the Archer SaaS Service Offering

1. Adherence To Standards of Protection. Archer will apply commercially reasonable efforts to carry out the following procedures to protect Customer Content. In fulfilling its obligations under this Exhibit, Archer may, from time to time, utilize methods or procedures ("**Processes**") similar to and substantially conforming to certain terms herein. Archer shall ensure that any such Processes are no less rigorous in their protection to Customer than the standards reflected in this Exhibit's terms set forth below and shall provide safeguards no less protective than those of the original terms of this Exhibit in all material respects. For the avoidance of doubt, where Customer is purchasing an Archer Insight or Archer Engage Service Offering, all terms of this Exhibit 2 apply to the Service Offering(s), not to Incidental Software (as defined below) controlled by Customer; Customer acknowledges and agrees that it is responsible for all appropriate information security and business continuity concerns related to Customer's use of Incidental Software.

2. Definitions.

2.1. "**Authorized Persons**" means Archer's employees, contractors, or other agents who need to access Customer Content to enable Archer to perform its obligations under the Agreement, and who are bound by confidentiality and other obligations sufficient to protect Customer Content in accordance with the terms and conditions of the Agreement.

2.2. "**Encryption**" is a process of using an algorithm to transform data into coded information to protect confidentiality.

2.3. "**Firewall**" is an integrated collection of security measures used to prevent unauthorized electronic access to a networked computer system.

2.4. "**Incidental Software**" means software that must be installed in Client's on-premises environment to enable Client to use the Service Offering(s). This section applies to Archer Engage and Archer Insight only. If Client is an on-premises Archer GRC Platform Software Client, Client acknowledges and agrees that Incidental Software must be downloaded, installed, managed, configured, and maintained by Client to use its on-premises installation of the Archer GRC Platform Software to enable Client to use the Service Offering(s). Client may use that software only (a) in connection with Client's use of the Service Offering(s), (b) for the Subscription Term, and (c) in accordance with the Agreement. If that software is subject to an accompanying license agreement, Client must comply with the terms of that license. If that software does not have an accompanying license agreement, then Archer's standard end user license agreement made generally available by Archer on its website applies.

2.5. "**Intrusion Detection Process**" (or "**IDP**") is a method of reviewing system events and Processes in near real time and, without unreasonable delay, alerting management to known patterns of behavior that indicate an intrusion is occurring or is likely to take place soon.

2.6. "**Security Incident**" means any loss of, or unauthorized or unlawful access to, acquisition of, use of, or disclosure of, Customer Content within the possession (*e.g.*, the physical or IT environment) of Archer or any Authorized Person.

3. Breach Notification and Remediation.

3.1. If Archer becomes aware of a Security Incident, Archer shall, in the most expedient time possible under the circumstances, notify Customer of the Security Incident and shall, subject to applicable laws, regulations, or a governmental request, provide Customer with details to the extent available about the Security Incident, including how it occurred and how Archer will address the Security Incident. In the event of a Security Incident, Archer and Customer shall cooperate in good faith to resolve any privacy or data security issues involving Customer Content, and to make any legally required notifications to individuals affected by the Security Incident. If there is a Security Incident involving Archer's systems or network, Archer shall:

3.2. Breach Notification. Within seventy-two (72) hours after the Security Incident notify Customer of the approximate date and time of the Security Incident and a summary of known, relevant facts and actions taken to rectify the Processes and address the Security Incident's effects.

3.3. Breach Remediation. Promptly implement reasonable measures necessary to address the security of Archer's systems and the security of Customer Content. If such measures include temporarily restricting access to any information, network or systems comprising the Service Offering to mitigate against further breaches, Archer shall promptly notify Customer of the restricted access, in advance of such restriction when possible but in all cases as soon as possible under the circumstances. Archer shall cooperate in good faith with Customer to allow Customer to verify Archer's compliance with its obligations under this clause.

4. Independent Control Attestation and Testing. Archer shall employ independent third-party oversight as follows:

4.1. Attestation. At least annually and at its own expense, Archer shall ensure that an audit of data center facilities where Customer Content is stored, processed, or transmitted by Archer is conducted according to appropriate industry security standards by an independent third party auditor and that such audit will result in the generation of an industry standard audit report (for example, SSAE-18 SOC 2, Type II, ISO 27001, or similar) ("**Audit Report**"). Upon Customer request and no more than once annually, Archer shall: (i) make good faith answers to an industry standard security questionnaire; and (ii) ensure that a copy of the most recent Audit Report pertaining to the Service Offering is available to customer. The availability of such Audit Report shall be made under a separate non-disclosure agreement mutually agreed upon by the parties.

4.2. Penetration Testing. At least annually and at its own expense, Archer shall engage a third-party testing service provider for network penetration testing of the infrastructure and systems used to provide the Service Offering and upon reasonable Customer request, Archer will provide a copy of the most recent executive summary pertaining to said testing.

4.3. Follow-up Inquiries. For clarification and the avoidance of doubt, to the extent such information has not otherwise been made available to Customer, Customer has the right to request clarifying information related to: Audit Reports; Archer's good faith answers to previously-answered industry standard questionnaires; executive summaries of third-party penetration testing reports related to the Service Offering; vulnerabilities of which the public is generally aware (such as zero-day vulnerabilities); and questions posed by regulators in accordance with applicable law which are not addressed by the foregoing ("**Follow-Up Inquiries**"). Follow-up Inquiries must be made in writing by Customer, and Archer will use commercially reasonable efforts to respond to Follow-up Inquiries in a timely manner given the nature and scope of such Follow-up Inquiries. Notwithstanding the foregoing, in no event shall Archer be obligated disclose information Archer reasonably deems: Archer proprietary information; information beyond the scope of the Service Offering as it relates to Customer; or information related to an ongoing (i.e., not yet remediated) security concern where the disclosure of such information has the potential to lead to a Security Incident.

5. Data Security. Archer shall use commercially reasonable efforts to carry out the following procedures to manage Customer Content as follows:

5.1. Information Classification and Logical Separation. If Customer discloses Customer's Content to Service Provider or if Service Provider accesses Customer's content as permitted by the Agreement, Customer Content shall be classified as Confidential and handled in accordance with the terms hereof. Archer will have no visibility at upload into the types of information stored on the Service Offering by Customer. Customer Content shall be logically separated such that there is no co-mingling of Customer Content with that of any other Service Provider customers.

5.2. Encryption of Information. Industry-standard encryption techniques (for example, public encryption algorithms such as IDEA and AES) shall be used at cipher strengths no less than 256-bit or equivalent for Customer Content. Archer shall use industry standard authentication practices to authenticate parties and secure messages and/or communications involving Customer Content, where applicable.

5.3. Cryptographic Key Management. Archer shall ensure that cryptographic keys are managed securely in accordance with control requirements and procedures which are consistent with industry best practices and shall ensure that Customer Content is protected against unauthorized access or destruction. Archer shall ensure that if public key infrastructure (PKI) is used, it shall be protected by 'hardening' the underlying operating system(s) and restricting access to certification authorities.

5.4. Data Access; **Transmission**. Archer shall make Archer-controlled applications and systems used to process or store Customer Content accessible only by those whose job responsibilities require such access. If transferred across the Internet, wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, Customer Content shall be protected using appropriate cryptography.

5.5. Event Logging.[1] For systems directly providing the Service Offering to Customer, Archer shall maintain logs of key events that may affect the confidentiality, integrity, and/or availability of the Service Offering to Customer and that may assist in the identification or investigation of material incidents and/or security breaches occurring in relation to Archer systems. The logs shall be retained for at least 90 days and protected against unauthorized changes (including, amending or deleting a log). Archer will monitor and log all system access to the Service Offering to produce a forensic trail that includes, but is not limited to, web server logs, application logs, system logs, and network event logs, as applicable to the Service Offering(s). Such logs are Archer confidential information but will be disclosed as necessary to comply with applicable law.

5.6. Disposition of Customer Content. In the event of termination of the Service Offering(s), Archer shall use industry standard techniques (such as those detailed by NIST 800-88) designed to prevent Customer Content from being exposed to unauthorized individuals as part of the decommissioning process.

6. Computer & Network Security. Archer shall use commercially reasonable efforts to carry out the following procedures to protect Customer Content:

6.1. Server Security. Computer systems comprising the Service Offering shall be dedicated solely to the provision of the Service Offering and not used by Archer for development and/or testing unless required to fulfill obligations within this Agreement.

6.2. Internal Network Segment Security. Data entering the Service Offering's network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.

6.3. External Network Segment Security. The Service Offering's connections to the Internet shall (a) have appropriate security measures and controls applied, and (b) the Archer SaaS, Archer Engage, and Archer Insight Service Offerings include an IDP that monitors data within the external network segment and information coming to Firewalls. Archer's IDP shall be designed to detect and report unauthorized activity prior to entering the Firewalls. Archer shall disable unnecessary network access points.

6.4. Network and Systems Monitoring. Archer shall actively monitor its networks and systems used to provide the Service Offering to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.

6.5. User Authentication. Archer shall implement Processes designed to authenticate the identity of its system users through the following means:

- **User IDs**. Each user of a system containing Customer Content shall be assigned a unique identification code ("**User ID**").
- **Passwords**. Each user of a system containing Customer Content shall use a unique password whose length, complexity, and age should be governed in accordance with industry best practices.

[1] For Engage for Vendors, Engage for Business Users, and Archer Insight, where Customer utilizes Incidental Software (if any) in connection with the Service Offering(s), Customer is responsible for monitoring and logging the use of the Incidental Software that is under Customer's control.

- **Two-Factor Authentication for Remote Access**. Remote access to systems containing Customer Content shall require the use of two-factor authentication.
- **Deactivation**. Archer User IDs shall be automatically deactivated after a technologically enforced number of unsuccessful log-in attempts. Interactive sessions shall be restricted or timed out after a technologically enforced period of inactivity. User IDs for Archer Personnel with access to Customer Content shall be deactivated promptly upon changes in job responsibilities that render such access unnecessary and during termination of employment.

6.6. Account Access. Archer shall provide account access to Archer Personnel on a least-privilege, need to know basis.

6.7. Malware Protection. Archer will install and run industry standard malware protection on all systems underlying the Service Offering. Anti-malware definition files shall be updated regularly in accordance with industry standards. For the avoidance of doubt, Customer remains responsible for protecting its own systems by installing, updating, and maintaining industry standard malware protection. For Engage for Vendors, Engage for Business Users, and Archer Insight, Customer is responsible for malware protection on all systems underlying the Incidental Software (if any) that is under Customer's control.

7. System Development.

7.1. Development Methodology and Installation Process.

- **Documented Development Methodology**. Archer shall ensure that development activities for Archer-developed software used in the provision of the Service Offering are carried out in accordance with a documented system development methodology.
- **Documented Deployment Process**. Archer shall ensure that new systems and changes to existing systems used in the provision of the Service Offering are deployed in accordance with a documented process.

7.2. Testing Process. Archer shall ensure that all reasonable elements of a system (i.e. application software packages, system software, hardware and services, etc.) shall be tested at all relevant stages of the systems development lifecycle before applicable system changes are promoted to the production environment.

7.3. Customer Content in Test Environments. Archer shall ensure that Customer Content is not used within Archer test environments without Customer's prior written approval.

7.4. Secure Coding Practices. Archer shall have secure development practices for itself and require the same of its coding vendors, if any, including the definition, testing, deployment, and review of security requirements.

8. General Security.

8.1. Point of Contact. Archer shall designate an account manager with whom Customer may coordinate as an escalation point beyond typical Service Offering customer support avenues available to Customer.

8.2. Data Center Facilities. The Service Offering shall be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physical environment secure from unauthorized access, damage, and interference. Archer will supply and maintain adequate heating/cooling; electrical power; server hardware; network infrastructure and bandwidth; physical security and access controls; and professional fire detection/suppression capability necessary to provide the Service Offering. Additional requirements specific to the data center facilities are:

- **Two-Factor Authentication**. Two-factor authentication shall be required for entry on access points that are designed to restrict entry and limit access to certain highly sensitive areas.
- **Limited Internet Access**. Archer Personnel shall have access to external email and/or the Internet only to the extent required by job function in support of the Service Offering.

- **CCTV Systems**. Closed circuit television (CCTV) systems and CCTV recording systems shall be used to monitor and record access to controlled areas.
- **ID Badges**. Identification badges showing the bearer's name, photographic likeness and organization to which he or she belongs shall be issued and required at data center facilities at all times.
- **Visitor Procedures**. Procedures for validating visitor identity and authorization to enter the premises shall be implemented and followed, including but not limited to an identification check, issuance of a clearly marked Visitor identification badge, host identity, purpose of visit, and recorded entry and departure times.

8.3. Change and Patch Management. Archer shall use commercially reasonable efforts to ensure that changes (including but not limited to emergency fixes, application patches, firmware updates, and similar) to its applications and infrastructure associated with the Service Offering are tested, reviewed, approved, and applied using an industry standard change management process that accounts for risks to Archer, its customers, and other such factors as Archer deems relevant. During the Subscription Term, Archer reserves the right to make modifications, including upgrades, patches, revisions or additions to the Service Offering.

8.4. Archer Personnel.

- **Background Screening**. Archer shall perform background checks in accordance with Archer screening policies on all Archer employees and consultants who are or will be supporting the Service Offering under this Agreement, to the extent permitted by applicable law.
- **Training**. Archer Personnel involved in the provision of the Service Offering shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided within one (1) month of Archer Personnel being engaged in the provision of the Service Offering or prior to Archer Personnel being given access to Customer Content.
- **Subcontractors**. Where applicable, Archer shall require subcontractors engaged in the provision of the Service Offering(s) (other than auxiliary services that facilitate the Service Offering(s) (e.g. guard service, media destruction, etc.)) to have in place and maintain a commercially reasonable business continuity program that complies with industry best practices.

9. Business Continuity Planning.

9.1. Archer shall ensure that the Service Offering business continuity plan ("**BCP**") capabilities include, at a minimum, a secure contingency site containing the hardware, software, communications equipment, and current copies of data and files necessary to perform Archer's obligations under this Agreement.

9.2. BCP Requirements. The BCP shall:
- Address the relocation of affected Archer Personnel to contingency locations and the reallocation of work;
- Require a remote contingency site with adequate security and capacity to provide the Service Offering in accordance with the obligations of this Agreement;
- Require Processes designed to ensure that Customer Content and other data necessary for the performance of the Service Offering are automatically copied to a remote contingency site;
- Include a description of the recovery process to be implemented following the occurrence of a disaster;
- Detail key resources and actions necessary to ensure that business continuity is maintained;
- Include a forty-eight (48) hour recovery time objective ("**RTO**") in which the Service Offering shall be recovered following the occurrence of a disaster; and
- Allow for the recovery of Customer Content at the remote contingency site in accordance with a twenty-four (24) hour recovery point objective ("**RPO**").

9.3. BCP Testing. At least annually and at its own expense, Archer will conduct a test of the BCP Plan. Upon reasonable request, Archer will provide an overview consisting of the date(s), scope, and outcome (on a succeed or fail basis) of the last test.

9.4. Backups. During the Term, Archer shall perform regular backups of Customer Content to assist Archer in recovery of the Service Offering(s) in the event of a Force Majeure event affecting the Service Offering(s). For

Engage for Vendors, Engage for Business Users, and Archer Insight where Customer utilizes Incidental Software (if any) in connection with the Service Offering(s), Customer is responsible for backups of the Incidental Software that is under Customer's control. The retention period for such backups shall be in accordance with Service Provider's backup retention policies, and Customer remains responsible for reinstating backups to the extent loss of Customer Content is not caused by Service Provider.

9.5. BCP Activation.

- **Notification**. In case of a Force Majeure Event that Archer reasonably believes will impact the Service Offering or its ability to perform its obligations under this Agreement, Archer shall, to the extent possible, promptly notify Customer of such Force Majeure Event. Such notification shall, as soon as such details are known, contain:
  - A description of the Force Majeure Event in question.
  - The impact the Force Majeure Event is likely to have on the Service Offering and Archer's obligations under this Agreement.
  - The operating strategy and the timetable for the utilization of the contingency site.
  - The timeframe in which Archer expects to return to business as usual.
  - Crisis management escalations affecting Customer Content.

- **Contact Points**. Archer Customer Support and/or Customer's Archer account manager shall coordinate with Customer's representative for the purpose of exchanging information and detailed, up-to-date status and on-going actions on and from the occurrence of a disaster. Customer shall make sure that its representative is always known to Archer Customer Support.